Wireless Technologies: *Beaming it to the Users*

Military Librarians Workshop

2004 Annual Conference

December 7, 2004

R. James King

Ruth H. Hooker Research Library

U.S. Naval Research Laboratory

Outline

- What is wireless technology?
- How is it being used?
- What is allowed in DoD?
- The Future…

What is wireless technology?

- A standard method of communication using broadcast-style methods
- Based upon several international standards either released or being developed

802.11a

- Supports speeds up to 54Mbps
- Operates in the 5GHz range
- Possible interference from radar and other military applications
- 300MHz total bandwidth available for use

802.11b – “Wi-Fi”

- Supports speeds up to 11Mbps
- Operates in the 2.4GHz range (also used by Industrial, Scientific and Medical fields)
- Possible interference from cordless phones, microwaves and Bluetooth devices
- 83MHz total bandwidth available for use

802.11g

- Extension of popular 802.11b
- Supports speeds up to 54Mbps
- Operates in the 2.4GHz range (also used by Industrial, Scientific and Medical fields)
- Possible interference from cordless phones, microwaves and Bluetooth
- 83MHz total bandwidth available for use

802.16 – “WiMax”

- Broadband Wireless Metropolitan Area Network
- Broadband speeds with cell tower ranges
- Operates in the 2.5GHz to 3.5GHz spectrum
- Standard being backed by over 140 companies including Intel
- Predicted to support 8% of all Internet users by 2008

Other Related Standards

- 802.15 – Wireless Personal Area Network
- Bluetooth – Short Range (2-10’) Wireless
- Intel ‘Centrino’ - 802.11b in chipset
- RFID – Radio Frequency Identification
- WPA – Wi-Fi Protected Access security

How is it being used?

- Handhelds & PDAs
- Office networks
- Home networks
- Military warfighter
- Supply chain
- Library Collection Management

NRL RFID Implementation

- Deployed 50,000+ digital tags to book and reference collection
- Finished initial tagging in ~6 months
- Allows shelf reading in a couple days
- Checks for weeding candidates, mis-shelved, holds, and ‘missing’ material with one pass
- Equipment needed:
  - Self-checkout upgrade
  - Cataloging station
  - Handheld reader with ‘triage’ cart

NRL Wireless LAN Deployment

- NRL Networking deployed ‘hot spots’ in conference center, cafeteria, and library
- Will run on external network allowing access to Internet, but not to internal LAN
- Library purchasing wireless-enabled laptops
- Equipment deployed but not yet activated

Wireless PDA Policies

Conflict between security and technological changes

- Security standards develop slower than wireless technologies.
- Technology changes continue to introduce new problems

Wireless PDA Policies

Specific DoD Wireless Policies:

- *Navy Wireless LAN Moratorium*
- *Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG)* – 8100.2 (12/5/03)
- *Pentagon Area Common Information Technology (IT)* – 9/25/2002
- *Wireless Security Technical Implementation Guide* (STIG), DISA, 12/3/2002

Wireless PDA Policies

Essentials from the Pentagon-area policy:

- Recognizes the pace of technology change by requiring an annual review.
- Does not apply to Sensitive Compartmented Information Facilities (SCIFs)
- Excludes Land Mobile, Emergency, and Tactical Radios and one-way receive only devices (e.g., devices with a wireless receiver and no transmitter)
- Requires punitive action for repeated violations of this policy that jeopardize the security of the Pentagon Area common IT Enterprise.

Wireless PDA Policies

Essentials from the Pentagon-area policy - prohibitions:

- connectivity to a classified network or computer
- Synchronization with IT devices that are not approved by a Designated Approving Authority (DAA)

Wireless PDA Policies

Essentials from the Pentagon-area policy - allowances:

- For **unclassified data** only
- In areas where unclassified information is electronically stored, processed, or transmitted
- In areas where classified information is electronically stored, processed, or transmitted unencrypted **when** there is a documented operational need.

Wireless PDA Policies

Other Policies that apply:

- DoD e-mail requirements apply to Wireless transmission - must have S/MIME encryption and PKI for Identification and Authentication (I&A)
- FIPS 140-1/2, overall Level 2 (Triple-DES or AES) standard) at minimum must be used for UNCLASSIFIED information.
- PEDS when connected directly (such as when synchronizing) to a DoD network may not be operating wirelessly at the same time.

Wireless PDA Policies

Antivirus Protection

- Antivirus software for PDAs now included in DoD CERT. Use is required!
  - Proactive prevention against future PDA viruses and Trojans
  - More antivirus programs for PDAs than there are viruses (Phage, Liberty/Crack)

Wireless PDA Policies

Personal Devices

- DoD Policy will forbid personally owned wireless devices from being connected to all DoD systems without the approval of the appropriate DAA. Likewise DoD-controlled wireless devices shall not be connected to DoD information systems unless approved of by the local DAA.

Wireless PDA Policies

Search for Balance

The DoD policy seeks to "establish a balanced approach for mitigating vulnerabilities and security risks while supporting the responsible introduction of new technologies into the workplace."

The Future… Location

- e911 – location information coded into all phones
- OnStar – location and situation based response to emergencies
- Instant Messaging – ability to know when at computer
- Interactive cell phones – instant virtual interest matching service

The Future… Flexible displays

The Future… Convergence

The Future…

- Better, more flexible devices
- Faster networks
- Enhanced security